Blockchain Technology Application for Electronic Voting Systems

K MANI[1], G Dhivya[2]
[1] *Karpagam Academy Of Higher Education India*

Keywords: Remote electronic voting; security; anonymity; transparencyBlockchain; smart contracts; mobile applications.

Abstract: Low voter turnout, limited access to polling locations, and mistrust of the voting process persist as ongoing challenges within the voting system. Addressing these issues, this paper introduces a pioneering solution: a blockchain-based remote electronic voting system. This system aims to empower users in creating their voting procedures, ensuring transparency throughout the voting process, and guaranteeing fault tolerance even in the event of hardware failures. Leveraging blockchain technology, renowned for its security and immutability, the proposed system establishes a decentralized and transparent voting process. Users can securely register their identities, cast anonymous votes, and modify their votes while the voting session remains open. Real-time access to voting results and a robust smart contract system further enhance the system's transparency and reliability. By eliminating the necessity for physical polling locations and enabling mobile voting, this system has the potential to bolster civic engagement and increase participation in the electoral process. While the implementation of blockchain-based electronic voting systems continues to evolve, this paper delineates the potential benefits and challenges associated with such systems, providing a promising path for the future of secure and transparent elections.

1. INTRODUCTION

One of the most important issues with the voting system continues to be low voter turnout. The event's limited duration and location, as well as mistrust of the voting process, are the causes of the poor voter turnout. The most promising method to get rid of these factors is remote electronic voting, which has to deal with the challenges of not only guaranteeing fault tolerance but also ensuring total security and defense against hacking for the entire system.

But as technology advances, new possibilities arise, altering the current circumstances. The issues with distant electronic voting will be resolved by the usage of blockchain technology. Therefore, the objective of the study is to create a blockchain-based remote electronic voting system that will enable users to meet the following requirements: the capacity to generate voting object lists, the capability of registering voters, the option to cast an anonymous ballot, the option to alter your vote while voting is still open, transparency of voting, guaranteeing the impossibility of changing vote outcomes on purpose, and fault tolerance assurance. People who use this voting system ought to be allowed to create their own voting procedures, including lists of candidates, eligibility requirements (allowing only residents of a certain jurisdiction to vote), the ability to vote anonymously, and the ability to change their minds at any point during the voting session. To make voting transparent, real-time access to results should be available to every user of a remote voting system. According to the assurance adjustments, infiltrations to alter a person's information in order to affect the voting process and its results should not occur.

According to the fault tolerance assurance, the system must continue to function even if a voting database device breaks down. Blockchain technology organizes blocks into a continuous chain. The foundation of it is distributed control. As a result, the blockchain serves as an information database. Users using anonymous networks are nodes. All conversations within the department are to accurately identify the source and destination; networks use cryptography. A network-wide consensus is reached to decide where a fact should be added to the ledger when a node desires to do so. The term 'block' refers to this arrangement.

The core tenet of blockchain technology is that all data is stored in copies or information-rich blocks on the devices of users linked to the blockchain network. Since there are more users on the blockchain network, the work is more reliable and of a higher standard, for it is totally transparent, changing every other record

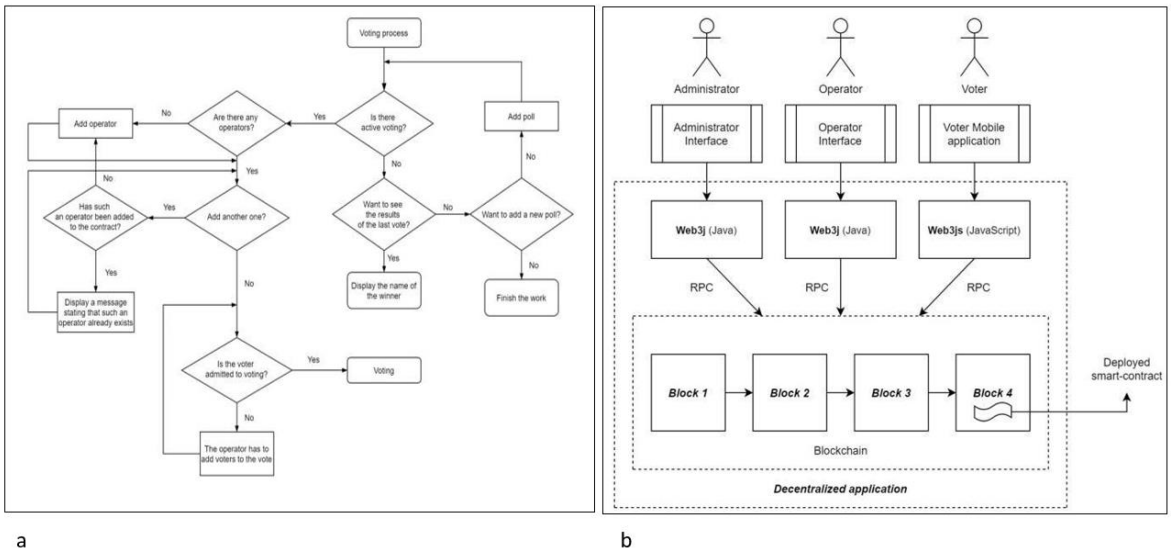

Fig.1. (a) Remote voting algorithm using smart contracts. (b) Decentralized Application

in the chain because each new block builds on the one before it [1]. Let's show that this is true.

Each block is composed of a current before it, a set of transactions, and some data. Depending on the Blockchain's goal, a block may include different types of data. A block's hash can be compared to a fingerprint. It identifies the block and all of its contents; it is always unique. The hash is computed after a block is formed. If anything inside the block is modified, the hash will change. In other words, hashes come in handy when it comes to spotting block modifications. A block is no longer the same block if the block's hash changes. The hash of the preceding block is the third component in each block. The Blockchain technology is more secure than a traditional ledger because every block includes the hash of the preceding block, (see Figure 1).

Every block owner is aware of the hash of the block before it. Consequently, according to Figure 1, Block 3 points to Block 2, and Block 2 points to Block 1. Being the first block, the Genesis block is unique in that it cannot refer to the prior block. It's referred to as a generating block.

The hash of Block 2 will change if we assume that Block 2 has been altered (falsified) (see Figure 2). Consequently, Block 3 and all succeeding blocks will become void because they no longer possess a valid hash of the block before them. Thus, changing one block invalidates all succeeding blocks. However, hashing by itself cannot prevent tampering.

Modern computers operate at incredibly high speeds, allowing for swift modifications to blocks and quick recalculations of hashes to restore the Blockchain's validity. To prevent this, Blockchain employs a 'proof of work' mechanism [1]. This method slows down new block production and significantly complicates altering existing blocks, as recalculating 'proof of work' for one block necessitates the same for all subsequent blocks. Hence, the proof of work and sharing of hashes form the bedrock of blockchain security. Additionally, decentralization plays a vital role in Blockchain's self-protection. Rather than relying on a centralized institution (peer-to-peer network), anybody can connect. Each user connected to this network receives a complete copy of the chain to verify its legitimacy.

Every node in the network receives copies of newly created blocks and conducts hash checks to ensure their validity. Once each node verifies that every detail in a block is in place, the network reaches consensus. This consensus distinguishes valid from incorrect blocks. To falsify a chain and achieve consensus, all modified blocks and those following in the chain must be altered, making it practically impossible to manipulate.

The benefits of decentralization, data immutability, preservation of all transactions through blockchain technology, are remarkable. These features allow blockchain to capitalize on its advantages and overcome hurdles. A recent advancement is the development of smart contracts.

By communicating pre-written conditions to all nodes, a smart contract connects Blockchain to the outside world [1]. This innovation eliminates the need for a notary public or other authorized intermediary, acknowledged by both parties.

Blockchain-based electronic voting systems have made headway in numerous established nations and gained acceptance not only at regional but also federal levels. For instance, after a successful test of a voting system for corporate shareholders in Estonia, West Virginia proposed the creation of a state-level blockchain-based voting platform for absentee voting. This system preserves anonymity and is more efficient [3].

Notable among private initiatives is the government pilot, creating an electronic voting platform allowing mobile voting while leveraging Blockchain's immutability and the security features of the latest smartphone technology. Voatz has successfully conducted live elections at city meetings, state party congresses, and student government elections [4]. Follow My Vote, though still in the demo stage, has gained widespread attention, aiming to establish a voting platform ensuring accurate results and election transparency without compromising voter privacy [5].

Kaspersky Lab stood out among Russian developers by developing the Blockchain- and encryption-secured Polys electronic voting technology [6]. Another attention-worthy project is the 'Active Citizen' project for conducting open referendums, developed at the request of the City Government in 2014. Moscow's voting system transitioned to Blockchain in November 2017, utilizing smart contracts for vote execution. The voting results impact departmental decisions and local ordinances for Moscow [7]. Despite several advances a block chain based voting system ha snot been implemented or adopted by any of the democratic countries.

2. BLOCKCAHIN BASED VOTING SYSTEM

The remote electronic voting system utilizes mobile communication. To participate in voting through this system, you need to install the mobile application on your device. The Blockchain-based remote electronic voting approach presented comprises the following steps:

Identify confirmation:

In order to use mobile voting, a citizen must initially establish their legal status in the country. This requires presenting their identity to the Operator—an impartial third party authorized to verify the user's identification and voting rights—by using the identity blockchain point and displaying an identity document. Consequently, only voters with the legal entitlement are permitted to vote, following this process to gain access to electronic voting.

The Central Election Commission (CEC) designates a specific time before the elections commence (for instance, during the presidential campaign) for verifying the voter's identity. Election organizers (Operators) solely conduct this procedure, making the system not entirely automated. However, the transparency of the identity card verification process remains intact.

Registration:

The user must possess an address space within the Blockchain technology to utilize it. This can be obtained by using an optical QR code scanner available in the mobile application. By scanning the QR code, the user establishes connection to the Blockchain.

The election process begins when a voter transfers a token representing their preferred candidate, similar to sending a conventional election token. Anonymity is maintained during this process as the cryptocurrency token is transferred from one wallet to another using encryption. The voter's token remains disconnected from their identification due to the absence of a unique identifier (QR code) on their mobile device.

The Election Administrator sets a time limit for the token, after which it either becomes invalid or, through a smart contract, self-destructs. The automated adjustment of the voting period impacts the functionality of the "Cast your vote" and "Change your vote" buttons in the user's mobile application. If a user logs into the mobile app before the voting period begins, the "Cast your vote" button is disabled. The voting options include "Cast your vote" and "Change your vote." If a user doesn't have sufficient time to cast their vote within the voting period, the "Cast your vote" button becomes inactive.

With this ballot distribution method, voters can cast their votes on election day after receiving their token before the polls open. When tokens are issued, it's clear whose vote they correspond to within the Blockchain network.

Viewing voting results and transactions is accessible through the mobile app by selecting "My transactions," enabling voters to confirm in real-time that their votes were accurately sent and securely recorded in the Blockchain. Additionally, after confirming the selection of their preferred candidate, an indecisive voter can anonymously modify their vote anytime until the voting period concludes.

After casting their ballot, voters can check the public transaction register and interim online voting results through the "All transactions" option in the mobile app. Post the voting deadline, voters can access the mobile application online to view the final voting results.

The system allows for straightforward voting with the "Cast Your Vote" button and a list of candidates with checkboxes. A smart contract ensures that all data entered into the remote electronic voting system is securely transferred into the blockchain systems.

A smart contract is a piece of programmable code [1] structured to store data hierarchically. In the voting system, it encompasses essential data: the list of authorized voters, election date, time, location, candidate list, and the votes cast for each candidate.

3. RESULTS

Improved voting process transparency: Eliminating the reliance on national election officials, notorious for biases in vote tabulation, is facilitated by real-time monitoring enabled by the technology. This enhances users' confidence in the system.

Commitment to voter anonymity: The specific ballot remains confidential until acknowledged by the voter, ensuring complete ownership.

Enhanced system reliability and security: Trustworthy vote results stored on the blockchain network increase data security. The system's security lies in its inability to be tampered with without affecting other users. Any attempt at data falsification requires access to all information-containing blocks across the decentralized Blockchain network, thwarting hacking attempts seen in computerized voting.

Promise of fault tolerance: Decentralization via Blockchain technology ensures each user device holds a copy of vote data, even if some devices malfunction, ensuring uninterrupted system functionality.

Increased civic engagement: Enabling early ballot casting online from any location is crucial, especially for absentee voters. This accessibility promotes higher participation rates, enhancing electoral rights' actual exercise.

Rise in effectiveness: The proposed remote voting technique minimizes the time, costs, and organizational challenges associated with traditional elections, reducing resource-intensive processes like ballot production, commission salaries, and facility rentals.

Quicker processing rate: The decentralized nature allows for real-time voting result transmission via the blockchain network, significantly reducing workload.

Accountability and limitations: Citizens are held responsible for their actions when using the program. Sharing personal mobile devices with installed voting applications is prohibited for security reasons, ensuring the integrity of the election process."

4. ENERGY ASSORTED

The primary objective of this project is to establish a secure voting environment, showcasing the potential for a dependable e-voting system employing blockchain technology. Decision-making within this system will be participatory, allowing every computer or mobile phone user to engage in e-voting. This inclusivity fosters increased visibility and accessibility of public opinion to managers and lawmakers, ultimately leading toward universal direct democracy [6].

Recent events, especially in rural and corrupt regions, have highlighted the vulnerability of individuals in traditional elections, where large-scale elections are both expensive and often witness low voter turnout due to various reasons like inaccurate listings or voter absence. Implementing electronic voting resolves many such issues.

The project focuses on developing a decentralized and adaptable e-voting protocol without a Trusted Third Party (TTP). Our scope is primarily limited to smaller-scale polls, like college elections, as the Ethereum network's scalability for nationwide elections requires further research.

The system operates via Ethereum's blockchain technology, enabling execution through any browser. By using smart contracts written in Solidity, we ensure a secure and verifiable voting mechanism, facilitating broader election influence.

Various successful implementations, like Estonia's e-voting system, serve as valuable models. These systems continue to evolve, maintaining

reliability and robustness with personal card readers and smart digital ID cards distributed by the government [10].

Furthermore, our project includes features such as petition creation via the parliament's website (http://rahvaalgatus.ee), highlighting technology's support for democracy. However, these systems are vulnerable to hacking attempts. Employing blockchain enhances security by preventing tampering and ensuring transparent transactions.

Switzerland's use of computerized voting systems and experimental blockchain-based systems in Sierra Leone and Russia illustrate diverse attempts at modernizing elections. While platforms like http://www.strawpoll.me/ demonstrate the accessibility of electronic voting, security concerns around voter identification and fraud persist, making it essential to further refine e-voting mechanisms for widespread use in official elections.

5. PROSPECTS

Because it allows greater security while maintaining system transparency and user privacy in comparison to services based on conventional databasesthe developed remote electronic voting system's sales market will have opportunities in a number of organisations that require remote voting..

It is important to note the following among the primary market segments for using Blockchain technology for remote voting:

• government agencies that oversee citizen voting;

• entities that use anonymous voting to reach significant decisions;

In several categories.

Registration Phase: The voter must first register themselves with their distinct identification and personal data, including name, roll number, and cellphone number. The database has all of this information.

Login: The voter tries to log in on their own after registering to vote. Voter logs on with a password during this phase. After logging in successfully, a voter must authenticate themselves in order to cast a ballot. OTP verification is used for real-time authentication to increase security.

Blockchain technology: This technology's security qualities are what make it so popular. Blockchain offers a transparent and safe environment. The voter message (the cast vote) is encrypted using an asymmetric encryption technique on the blockchain. Blockchain offers a public key, and the host has the private key. Ledger uses public key for verification purposes.

Ethereum Network: The Ethereum network offers a structure for the development and storage of blockchains. Each block is formed, and the information related to it is kept in an encrypted ledger. Because these newly produced blocks are dispersed among nodes, the system has a high fault tolerance.

6. CONCLUSIONS

It is necessary to conduct online identity blockchain-based architecture to be fully automated. After then, there is no question individual delivered used devic. In this work, we presented a novel, blockchain-based electronic voting system that ensures voters' privacy while enabling secure and affordable elections. In contrast to earlier research, we have demonstrated that the blockchain technology presents a fresh opportunity for democratic nations to move away from the pen and paper election system and towards a more time- and cost-effective election system while enhancing the security features of the current system and providing new opportunities for transparency.

In both political and academic areas, there is ongoing debate over electronic voting. Despite the fact that there are a few excellent instances, failed to fulfil or had significant usability and scalability problems [8]. Contrarily, blockchain-based e-voting solutions, like the one we created using smart contracts and the Ethereum network, address (or may address with pertinent modifications) almost all of the security issues, and the accuracy of the tally.

Although there is a lot of potential in blockchain technology, much more research is needed before it can be said to have reached its full potential. To make the underlying blockchain technology more capable of supporting more sophisticated applications, a concentrated effort is required.

critical integration technological equipping people, and public regarding use of new technologies.

REFERENCES

Moore, R., Lopes, J., 1999. Paper templates. In Zaninotto, 28 April 2016. "The Blockchain Explained to Web Developers, Part 1: The Theory" You may access this at: https://marmelab.com/blog/2016/04/28/blockchain-for-web- developersthe-theory.html.

Overview of blockchain technology's use in public administration, Solodkiy S. Easily accessible at: https://medium.com/ @ slavasolodkiy / overview-applications-of-blockchain-technology-in-government-ac53602cec7f (Accessed on April 9, 2019). The Russian.

Galaburdina A. "USA Introduces Blockchain For Voting In Elections." Available at: https://jourtify.com/ssha-vnedrjaetblokchejn-dlja-golosovanija-na-vyborah/. (Viewed on April 09, 2019). (In Russian.

Voting Redefined [4]. Accessed on April 09, 2019 at: https://voatz.com.

Reasons to Vote Online. Accessed on April 09, 2019 at https://followmyvote.com.

Shmyrova V. A voting platform powered by blockchain has been developed by "Kaspersky."(Accessed April 9, 2019) Available at: http://www.cnews.ru/news/top/2017-11-27_kasperskij_vynes_na_narodnyj_sud_izbiratelnuyu. In Russian.

On the blockchain, a "Active Citizen." (17 November 2017). Accessed on April 09, 2019 at https://ag.mos.ru/blockchain. In Russian